JACQUES TITS

Les groupes simples de Suzuki et de Ree

Séminaire N. Bourbaki, 1961, exp. n° 210, p. 65-82

<http://www.numdam.org/item?id=SB_1960-1961__6__65_0>

Séminaire BOURBAKI
13e année, 1960/61, n° 210

LES GROUPES SIMPLES DE SUZUKI ET DE REE

par Jacques TITS

1. Les groupes B_2^* , G_2^* et F_4^* ([1]).

On commencera par rappeler, à titre de comparaison, le principe de la construction des formes non normales (i. e. non du type "Tôhoku") de groupes simples, à partir des formes normales.

Soient K un corps de caractéristique p (= ou $\neq 0$) , $\mathcal{G}$ une algèbre de Lie complexe semi-simple, Σ un système de racines simples de $\mathcal{G}$, Δ le schéma de Dynkin de $\mathcal{G}$ (dans lequel on suppose qu'on peut discerner les racines de longueurs différentes), G le "groupe du Tôhoku" [3] de type $\mathcal{G}$ sur K , et soient $x_a(t)$, $\mathfrak{X}_a = \{x_a(t)\}$ et $h(\chi)$ définis comme dans [3]. A tout automorphisme π de Δ correspond une permutation isométrique de Σ qui s'étend en une permutation isométrique de l'ensemble de toutes les racines, laquelle sera encore désignée par π . On notera α_π l'automorphisme de G défini par

$$x_a(t) \rightsquigarrow x_{\pi(a)}(t) \qquad (a \in \Sigma)$$

$$h(\chi) \rightsquigarrow h(\chi') \quad \text{avec} \quad \chi'(\pi(a)) = \chi(a) \qquad .$$

Pour toute racine a , cet automorphisme transforme $\mathfrak{X}_a$ en $\mathfrak{X}_{\pi(a)}$. Par abus de langage, les automorphismes de G qui sont le produit d'un α_π par un automorphisme intérieur seront dits birationnels.

A tout endomorphisme θ de K , on peut associer un endomorphisme α_θ de G défini par

$$x_a(t) \rightsquigarrow x_a(t^\theta) , \qquad h(\chi) \rightsquigarrow h(\chi^\theta) \qquad ([2]) \qquad .$$

([1]) Ce paragraphe et les deux suivants s'inspirent directement de deux articles encore inédits de R. REE [4] et [5], qui nous a aimablement permis de faire usage de ses manuscrits.

([2]) Les automorphismes de K sont notés exponentiellement ; à part cela, toutes les applications (et en particulier les automorphismes de G) opèrent à gauche.

Tout endomorphisme, produit d'un endomorphisme birationnel par α_θ sera dit *appartenir à* θ.

Si K est une extension galoisienne de groupe Γ d'un corps L, une *L-forme* de G peut être définie comme le groupe des éléments fixes d'un groupe d'automorphisme $\lambda(\Gamma)$ de G, image de Γ par un monomorphisme $\lambda : \Gamma \to \mathrm{Aut}\,(G)$ (groupe des automorphismes de G) tel que $\lambda(\gamma)$ appartienne à γ pour tout $\gamma \in \Gamma$. En particulier, à tout monomorphisme $\mu : \Gamma \to \mathrm{Aut}\,(\Delta)$, on peut faire correspondre une L-forme de G, à l'aide du monomorphisme λ défini par

$$\lambda(\gamma) = \alpha_{\mu(\gamma)} \cdot \alpha_\gamma \quad .$$

Les formes de D_4 et E_6, qui ont été considérées par D. HERTZIG, R. STEINBERG [8] et l'auteur [11] et [12], sont de ce type.

Si on fait abstraction des longueurs des racines, trois schémas de Dynkin acquièrent un automorphisme π d'ordre 2 ; ce sont les schémas de B_2, G_2 et F_4. A cet automorphisme, correspond une permutation de Σ qui conserve les angles entre paires de racines (mais non les longueurs de celles-ci), laquelle s'étend en une permutation de l'ensemble de toutes les racines qui jouit de la même propriété, et qu'on désignera encore par π. Dans certains cas particuliers, on peut encore lui associer un automorphisme, ou plus généralement un endomorphisme, non plus "birationnel" mais "rationnel" de G. De façon précise, si $\mathcal{S} = B_2$ ou F_4 (resp. G_2) et $p = 2$ (resp. 3), un calcul simple montre qu'il existe un endomorphisme α_π de G défini par

$$x_a(t) \rightsquigarrow x_{\pi(a)}(t^{\ell(a)}) \qquad (a \in \Sigma)$$

$$h(\chi) \rightsquigarrow h(\chi') \quad \text{avec} \quad \chi'(\pi(a)) = \chi(a)^{\ell(a)} \quad ,$$

où $\ell(a) = 1$ ou p selon que a est une racine "longue" ou "courte". Il est clair que $\alpha_\pi^2 = \alpha_\varphi$ où $\varphi : k \rightsquigarrow k^p$ est le Frobenius de K. Supposons que K possède un endomorphisme σ tel que $\sigma^2 = \varphi$. Alors $\alpha = \alpha_\pi^{-1} \cdot \alpha_\sigma$ est un automorphisme involutif ($\alpha^2 = 1$) du groupe $\alpha_\sigma^{-1}(\alpha_\sigma(G) \cap \alpha_\pi(G))$. En particulier, si K est parfait, φ, σ, σ_π et α_σ sont surjectifs, et α est un automorphisme de G (3). Dans tous les cas, on notera G^* ($= B_2^*$, G_2^* ou F_4^*) le groupe des éléments g de G tels que $\alpha_\pi(g) = \alpha_\sigma(g)$ (éléments invariants par α).

(3) Seul ce cas est considéré par R. REE. Certains des résultats exposés concernant le cas non parfait ont été vérifiés hâtivement ; on espère qu'ils sont néanmoins corrects.

Soient U_+ (resp. U_-) le sous-groupe de G engendré par les $\mathfrak{X}_a$ (resp. les $\mathfrak{X}_{-a}$) $(a \in \Sigma)$, et $U_+^* = U_+ \cap G^*$ (resp. $U_-^* = U_- \cap G^*$). On a alors le théorème suivant :

THÉORÈME 1. - Si K a plus de $p(=2$ ou $3)$ éléments, le groupe engendré par U_+^* et U_-^*, qui n'est autre que le groupe dérivé $G^{*\prime}$ de G^*, est simple. De plus, $F_4^* = F_4^{*\prime}$, $B_2^*/B_2^{*\prime} \cong K^*/K^{*\sigma}$ (en particulier, $B_2^* = B_2^{*\prime}$ si K est parfait), et $G_2^*/G_2^{*\prime} \cong K^*/M$, où M est un sous-groupe de K^* qui contient K^{*2} et -1 (4).

La partie de ce théorème qui concerne B_2^* et G_2^* sera démontrée plus loin, à partir d'une définition d'ailleurs quelque peu différente de ces groupes. Pour ce qui concerne F_4^*, on renverra à [5].

2. Décomposition cellulaire.

Les notations étant celles du paragraphe 1, soient W le groupe de Weyl de $\mathfrak{S}(=B_2$, F_4 ou $G_2)$, $\omega(w)$ $(w \in W)$ défini comme dans [3], H le groupe formé par les $h(\chi)$, Ω le groupe engendré par H et les $\omega(w)$, $\varpi : \Omega \to W$ l'homomorphisme de noyau H défini par $\omega(w) \rightsquigarrow w$, W^* le groupe des éléments de W invariants par π, $H^* = H \cap G^*$, $H_0^* = H \cap G^{*\prime}$, $\Omega^* = \Omega \cap G^*$, $\Omega_0^* = \Omega \cap G^{*\prime}$.

Il est clair que $\varpi(\Omega^*) \subseteq W^*$. En fait, on a le théorème suivant :

THÉORÈME 2. - $\varpi(\Omega^*) = \varpi(\Omega_0^*) = W^*$. Autrement dit, $\Omega^*/H^* \cong \Omega_0^*/H_0^* \cong W^*$.

La démonstration se fait en construisant explicitement pour tout $w \in W^*$ un $\omega(w)$ dans $G^{*\prime}$ (les trois cas, B_2, F_4, G_2, se traitant séparément). Dans la suite, on supposera toujours que les $\omega(w)$ $(w \in W^*)$ sont choisis de cette façon.

Quel que soit $w \in W$, on posera $U_+^w = U_+ \cap \omega(w).U_-.\omega(w)^{-1}$, et, lorsque $w \in W^*$, $U_+^{*w} = U_+^* \cap \omega(w).U_-^*.\omega(w)^{-1}$. Tout élément $g \in G$ peut être mis, d'une et une seule façon, sous la forme d'un produit $u'.\omega.u$, avec $u \in U_+$, $\omega \in \Omega$ et $u' \in U_+^{\varpi(\omega)}$ (théorème 2 de [3]). D'autre part, α_π et α_σ envoient chacun des groupes H, U_+, U_- et Ω dans lui-même (pour H, U_+ et U_- c'est évident ; pour Ω, cela résulte de ce que Ω est le normalisateur de H, et H le centralisateur de $\alpha_\pi(H)$ et de $\alpha_\sigma(H)$) ; il s'ensuit que si $g = u'.\omega.u$ appartient

---

(4) Il n'est pas impossible que $M = K^*$ (d'où $G_2^* = G_2^{*\prime}$) quel que soit K.

à G^* , il en est de même de u , u' et ω . Par conséquent,

THÉORÈME 3. – Tout élément de G^* (resp. $G^{*\prime}$) peut être mis, d'une et une seule façon, sous la forme d'un produit $u'.\omega.u$, avec $u \in U_+^*$, $\omega \in \Omega^*$ (resp. Ω_0^*) et $u' \in U_+^{*\varpi(\omega)}$.

Nous donnerons encore, pour chacun des groupes B_2^* , G_2^* et F_4^* , quelques indications sur la structure de W^* , U_+^* , H^* et H_0^* .

Soit $\mathfrak{G} = B_2$ (resp. G_2) . W^* se compose alors de l'identité et de l'opération w_0 qui transforme chaque racine en son opposée. $\omega(w_0)$ échange U_+^* et U_-^* , donc $G^* = U_+^*.H^*.\omega(w_0).U_+^* \cup U_+^*.H^*$, en vertu du théorème 3. Il en résulte que G^* est doublement transitif sur l'espace $\Gamma = G^*/U_+^*.H^*$, des classes latérales à gauche de $U_+^*.H^*$ dans G^*. En effet, on peut identifier canoniquement Γ à la réunion $U_+^* \cup \{\infty\}$ de U_+^* et d'un point ∞ , image de l'élément neutre, et le sous-groupe U_+^* de G^* opère transitivement sur lui-même et conserve ∞ . Nous retrouverons plus loin (paragraphes 4, 5, 6) cette représentation doublement transitive de G^* . Le sous-groupe H^* est isomorphe au groupe multiplicatif K^* de K ; l'isomorphisme peut être établi de telle façon que H_0^* corresponde au sous-groupe $K^{*\sigma}$ de K^* (resp. à un sous-groupe M satisfaisant aux conditions du théorème 1). U_+^* est nilpotent de classe 2 (resp. 3) et les quotients de sa série centrale ascendante sont tous isomorphes au groupe additif K^+ (la structure précise de U_+^* sera donnée au paragraphe 6). Si on désigne par a et b les racines simples, a étant la plus courte, on a, pour une normalisation convenable des $x_r(t)$,

$$U_+^* = \{x_a(t).x_b(t^\sigma).x_{a+b}(u).x_{2a+b}(t^{\sigma+2} + u^\sigma)\} \qquad (t\ ,\ u \in K)$$

$$(\text{resp.} \quad x_a(t).x_b(t^\sigma).x_{a+b}(u).x_{2a+b}(v).x_{3a+b}(u^\sigma - t^{\sigma+2}).x_{3a+2b}(v^\sigma - t^{2\sigma+2}) \qquad (t\ ,\ u\ ,\ v \in K)) \quad .$$

Soit $\mathfrak{G} = F_4$. W^* est alors un groupe diédrique d'ordre 16 . H^* est isomorphe à $K^* \times K^*$. De plus [5], il existe des sous-groupes $\mathfrak{X}_i$ et

---

([5]) Les propriétés suivantes ne sont pas énoncées par R. REE, mais se déduisent assez aisément de ses résultats.

$\mathfrak{y}_i$ $(i = \pm 1 , \pm 2 , \pm 3 , \pm 4)$, respectivement isomorphes à K^+ et à l'"unipotent" U_+^* de B_2^* , et jouissant de propriétés tout à fait analogues à celles des $\mathfrak{x}_r$ des groupes du Tôhoku, telles que, par exemple :

$\mathfrak{x}_i$ et $\mathfrak{y}_i$ sont invariants par R^* ;

les automorphismes intérieurs correspondant aux éléments de Ω permutent les $\mathfrak{x}_i$ et les $\mathfrak{y}_i$ de la même façon que les automorphismes euclidiens de la figure 1 permutent les demi-droites qui la composent (on voit que le "schéma de Dynkin" de F_4^* est un trait sextuple, ce qui rompt un peu la monotonie !) ;

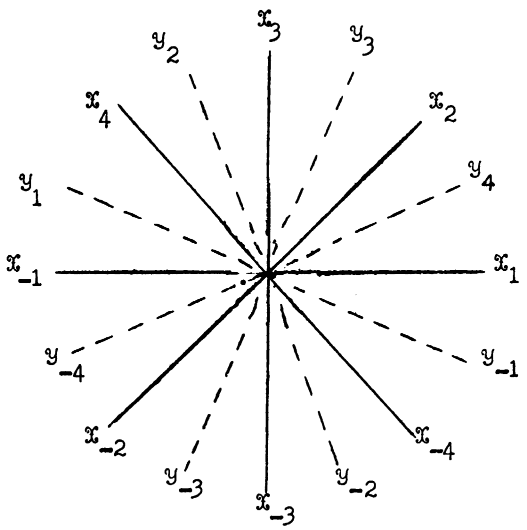

Fig. 1

si j groupes $\mathfrak{Z}_1 , \ldots , \mathfrak{Z}_j$, choisis parmi les $\mathfrak{x}_i$, $\mathfrak{y}_i$, correspondent à toutes les demi-droites de la figure 1 contenues dans un angle aigu ("cône convexe") Θ , tout élément du groupe U_Θ qu'ils engendrent peut être mis, d'une et une seule façon, sous la forme d'un produit $z_1 . z_2 \ldots z_j$, avec $z_m \in \mathfrak{Z}_m$; si Θ et Θ' désignent deux angles aigus, $U_{\Theta \cap \Theta'} = U_\Theta \cap U_{\Theta'}$;

U_+ est engendré par les $\mathfrak{x}_i$, $\mathfrak{y}_i$ $(i > 0)$;

pour tout i , $\mathfrak{x}_i$ et $\mathfrak{x}_{-i}$ (resp. $\mathfrak{y}_i$ et $\mathfrak{y}_{-i}$) engendrent un groupe isomorphe à $PSL_2(K)$ (resp. à $B_2^{*\prime}$) ;

si G_x^* (resp. G_y^*) désigne le groupe engendré par U_+ et $\mathfrak{x}_{-1}$ (resp. $\mathfrak{y}_{-1}$) , les ensembles G^*/G_x^* et G^*/G_y^* constituent, avec la relation d'incidence usuelle [10], un octogone généralisé (cf. [12], Appendice) ; on a ainsi une "interprétation géométrique" de F_4^* comme groupe d'automorphismes de cet octogone ; etc.

3. Groupes finis.

Soit K le corps fini de $q = 2^n$ (resp. 3^n) éléments. On voit aisément que le Frobenius $x \rightsquigarrow x^2$ (resp. x^3) possède une racine carrée, d'ailleurs unique, si et seulement si $n = 2m + 1$. Dans ce cas, on peut définir les groupes finis B_2^*

et F_4^* (resp. G_2^*), qui sont simples dès que $m > 0$, en vertu du théorème 3 (dans le cas de G_2, il faut remarquer que, en raison de l'hypothèse faite sur n, -1 n'est pas un carré dans K, d'où il résulte que -1 et K^{*2} engendrent K^*). Les ordres $o(G^*)$ de ces groupes se calculent aisément à partir des résultats du paragraphe 2, et on trouve

$$o(B_2^*) = q^2 . (q^2 + 1) . (q - 1) \ ,$$

$$o(G_2^*) = q^3 . (q^3 + 1) . (q - 1) \ ,$$

$$o(F_4^*) = q^{12} . (q^6 + 1) . (q^4 - 1) . (q^3 + 1) . (q - 1) \ .$$

On constate que $o(B_2^*)$ n'est pas divisible par 3, propriété qui n'est partagée par aucun autre groupe fini simple connu. R. REE note qu'on peut montrer que les G_2^* sont aussi de nouveaux groupes simples en utilisant le fait que $o(G_2^*)$ est divisible par 8 et non par 16. Enfin, on peut s'attendre à ce que la méthode d'Artin donne un résultat analogue pour F_4^*. Les B_2^* sont les groupes de SUZUKI [9] (cf. le numéro 4.3).

4. Une définition géométrique des groupes B_2^*.

4.1. - Dualité dans les "complexes linéaires" en caractéristique 2. - On emploiera à plusieurs reprises la notation abrégée suivante : "Un espace projectif $\Xi(\xi_0, \xi_1, \dots)$" = "Un espace projectif Ξ dans lequel on se donne un système de coordonnées homogènes $\xi_0, \xi_1, \dots$". D'autre part, une variété quelconque sera toujours assimilée à l'ensemble de ses points rationnels sur K.

Soient K un corps de caractéristique p et $E(x_0, x_1, x_2, x_3)$ un espace projectif à 3 dimensions sur K. Les droites de E peuvent être repérées au moyen de leurs "coordonnées de Plücker" p_{ij} satisfaisant à la relation $p_{01} . p_{23} + p_{02} . p_{31} + p_{03} . p_{12} = 0$. Considérons l'ensemble ("complexe linéaire") L des droites telles que $p_{01} = p_{23}$. Elles sont représentées, dans un espace projectif à 4 dimensions $D(p_{01}, p_{02}, p_{03}, p_{12}, p_{31})$, par les points d'une hyperquadrique V, d'équation

$$p_{01}^2 + p_{02} . p_{31} + p_{03} . p_{12} = 0 \ .$$

Supposons à présent que la caractéristique p de K soit égale à 2.

Les hyperplans tangents à V se coupent alors en un point, de coordonnées $p_{02} = p_{03} = p_{12} = p_{31} = 0$, ce qui permet de définir (par "projection" à partir de ce point), une injection "rationnelle" de V dans un espace projectif $F(y_0, y_1, y_2, y_3)$, par

$$(p_{01}, p_{02}, p_{03}, p_{12}, p_{31}) \rightsquigarrow (y_0 = p_{02}, y_1 = p_{31}, y_2 = p_{03}, y_3 = p_{12}) .$$

Les coordonnées de Plücker des droites de F seront notées q_{ij}. A l'ensemble des droites de L qui contiennent un point donné $(x_0, \dots, x_3)$ de E correspond une droite de V, donc une droite de F dont les coordonnées de Plücker sont, d'après un calcul élémentaire,

$$q_{01} = q_{23} = x_0 \cdot x_1 + x_2 \cdot x_3 , \qquad q_{02} = x_0^2 , \qquad q_{03} = x_2^2 ,$$

$$q_{31} = x_1^2 , \qquad q_{12} = x_3^2 ,$$

et qui, en particulier, appartient à l'ensemble de droites M d'équation $q_{01} = q_{23}$. Ainsi est établie entre (E, L) et (F, M) une sorte de dualité, constituée par deux injections $\delta : L \to F$ et $\delta' : E \to M$, telles que si $\underset{\sim}{x}$ et d désignent respectivement un point de E et une droite appartenant à L, les propriétés $\underset{\sim}{x} \in d$ et $\delta(d) \in \delta'(\underset{\sim}{x})$ soient équivalentes.

Désignons par $G(E, L)$ (resp. $G(F, M)$) le groupe, isomorphe à $P\Gamma Sp_4(K) = B_2$ du Tôhoku, des projectivités de E conservant L (resp. des projectivités de F conservant M). La "dualité" entre (E, L) et (F, M) "induit" un monomorphisme $\delta^* : G(E, L) \to G(F, M)$, défini par $\delta^*(g)\,(\delta'(d)) = \delta'(g(d))$, pour tout $g \in G(E, L)$ et toute droite $d \in L$.

4.2. - <u>La "polarité"</u> f. - Supposons à présent que le Frobenius de K possède une racine carrée σ, et considérons l'application semi-linéaire $f : E \to F$ définie par

$$(x_0, \dots, x_3) \rightsquigarrow (y_0 = x_0^\sigma, \dots, y_3 = x_3^\sigma) .$$

Du numéro 4.1, il résulte immédiatement que si $\underset{\sim}{x}$ et $\underset{\sim}{x}'$ sont des points de E, la relation " $f(\underset{\sim}{x})$ appartient à la droite $\delta'(x')$ " est symétrique ; f apparaît ainsi comme une sorte de polarité. On désignera par Γ l'ensemble des points $\underset{\sim}{x}$ tels que $f(\underset{\sim}{x})$ appartienne à sa "polaire" $\delta'(\underset{\sim}{x})$.

Introduisons à présent, dans E privé du plan $x_0 = 0$ ("plan à l'infini"), des coordonnées non homogènes $x = x_2/x_0$, $y = x_3/x_0$, $z = x_1/x_0$. Un calcul élémentaire montre que Γ se compose du point $x_0 = x_2 = x_3 = 0$, qu'on désignera par $\underset{\sim}{\infty}$, et de l'ensemble $\Gamma - \{\underset{\sim}{\infty}\}$, entièrement "à distance finie", d'équation

(4.2.1) $$z = x.y + x^{\sigma+2} + y^{\sigma} \quad .$$

4.3. Les groupes G^* et G_0^* . – On voit aisément qu'il existe un monomorphisme $f^* : G(E , L) \to G(F , M)$ défini par $f^*(g)\ (f(\underset{\sim}{x})) = f(g(\underset{\sim}{x}))$, pour tous $\underset{\sim}{x} \in E$ et $g \in G$.

On désignera par $G^*(f)$ le groupe des éléments $g \in G(E , L)$ tels que $f^*(g) = \delta^*(g)$ (groupe des projectivités "conservant f ") ; $G^*(f)$ n'est autre que le groupe B_2^* (le lien entre les deux définitions est apparent). Il est clair que $G^*(f)$ est contenu dans le groupe de toutes les projectivités de E qui conservent l'ensemble Γ , lequel sera désigné par G^* (en fait, $G^*(f) = G^*$: voir plus loin). Le groupe des éléments de G^* , dont le déterminant est une puissance 4e, sera noté G_0^* .

Les projectivités

$$t_{a,b} : (x , y , z) \rightsquigarrow (x + a , y + b + a^{\sigma} x , z + ab + a^{\sigma+2} + b^{\sigma} + ay + a^{\sigma+1}x + bx) \quad (a , b \in K) ,$$

$$h_k : (x , y , z) \rightsquigarrow (kx , k^{\sigma+1} y , k^{\sigma+2} z) \qquad (k \in K^*) ,$$

$$\omega : (x_0 , x_1 , x_2 , x_3) \rightsquigarrow (x_1 , x_0 , x_3 , x_2) ,$$

appartiennent à G^* . Pour $t_{a,b}$ et h_k , cela résulte d'un calcul facile; quant à la projectivité ω , il est immédiat qu'elle appartient à $G^*(f)$ (6). De plus, $t_{a,b}$ et $\omega \in G_0^*$, tandis que $h_k \in G_0^*$ si et seulement si $k \in K^{*\sigma}$. Enfin, on vérifie aisément que $\{t_{a,b}\} = T^*$ et $\{h_k\} = H^*$ sont des groupes.

LEMME 1. – Si K a plus de deux éléments, les h_k sont les seuls éléments de G^* conservant les deux points $\underset{\sim}{\infty}$ et $x = y = z = 0$.

DÉMONSTRATION. – Une projectivité conservant $\underset{\sim}{\infty}$ et Γ conserve le plan $x_0 = 0$, qui est en effet le seul plan contenant $\underset{\sim}{\infty}$ dont l'intersection avec Γ se réduit à ce point. Il s'ensuit qu'une projectivité conservant Γ , $\underset{\sim}{\infty}$ et $x = y = z = 0$

(6) On peut aussi vérifier par un calcul direct que $\omega \in G^*$. Le seul point quelque peu délicat de la démonstration consiste à établir que, sur Γ , $z = 0$ implique $x = y = 0$, or cela résulte immédiatement de la relation $y^{\sigma+1} = xz^{\sigma} + z(x^{\sigma+1} + y)$, conséquence de 4.2.1.

est une transformation linéaire représentée par une substitution linéaire et homogène sur x , y , z . Tenant compte du fait que Γ et $\underset{\sim}{\infty}$ sont conservés, on voit que si on effectue cette substitution dans la fonction $z + xy + x^{\sigma+2} + y^{\sigma}$, celle-ci doit être multipliée par une constante, mais il en est alors de même de ses "composantes homogènes" z , xy , $x^{\sigma+2}$, y^{σ} , en vertu de l'indépendance linéaire des endomorphismes multiplicatifs de K (cf. [2], paragraphe 7, n° 5) (on utilise ici le fait que $K^* \neq F_2$, puisqu'il faut supposer que les endomorphismes 1 , 2 , σ et $\sigma + 2$ sont tous différents entre eux). Par conséquent, la projectivité en question est de la forme $(x , y , z) \rightsquigarrow (k_1 x , k_2 y , k_3 z)$, et la démonstration s'achève par un simple calcul.

THÉORÈME 4. - Le groupe G_0^* (et a fortiori G^*) est doublement transitif sur Γ . Si K a plus de deux éléments, G^* (resp. G_0^*) est engendré par les projectivités $t_{a,b}$ $(a , b \in K)$, h_k $(k \in K^*)$ (resp. $K^{*\sigma}$) et ω (8). Tout élément de G^* peut être mis, d'une et une seule façon, sous l'une des deux formes $t_{a,b} . h_k$ ou $t_{a,b} . h_k . \omega . t_{c,d}$ $(a , b , c , d \in K , \; k \in K^*)$. Enfin, $G^*/G_0^* \cong K^*/K^{*\sigma}$.

DÉMONSTRATION. - Le groupe engendré par les $t_{a,b}$, les h_k $(k \in K^{*\sigma})$ et ω est doublement transitif sur Γ ; en effet, le sous-groupe T^* , qui conserve $\underset{\sim}{\infty}$, est transitif sur $\Gamma - \{\underset{\sim}{\infty}\}$, et ω "bouge" $\underset{\sim}{\infty}$. Le théorème est alors une conséquence immédiate du lemme 1 et du fait que T^* est simplement transitif sur $\Gamma - \{\underset{\sim}{\infty}\}$.

COROLLAIRE. - $G^*(f) = G^*$.

Il suffit de vérifier que $t_{a,b}$, h_k et ω appartiennent à $G^*(f)$.

REMARQUE. - On notera que le théorème 4 a été établi sur la base de la seule définition analytique (4.2.1) de Γ , sans même faire intervenir f (si on tient compte de la note (7)).

4.4. Propriétés de Γ . Calottes. - L'équation (4.2.1) montre que toute droite passant par $\underset{\sim}{\infty}$ et non contenue dans le plan $x_0 = 0$ recoupe Γ en un et un seul point. Tenant compte de l'"homogénéité" de Γ (théorème 4), on en déduit immédiatement la

PROPOSITION 1. - Toute droite de E coupe Γ , en 0 , 1 ou 2 points. Les droites passant par un point donné de l'ensemble Γ et qui ne le recoupent pas

(8) C'est essentiellement la définition de SUZUKI [9] du groupe B_2^* .

ailleurs (tangentes) forment un plan.

COROLLAIRE. - *Lorsque* $K = F_q$ *est le corps fini de* $q = 2^{2m+1}$ *éléments,* Γ *est formé de* $q^2 + 1$ *points.*

Désignons par $E_{r,q}$ l'espace projectif à r dimensions sur F_q ($q = p^n$, p quelconque). Un ensemble de N points de cet espace est appelé une N-*calotte* si toute droite le rencontre en 0, 1 ou 2 points. Les ensembles de ce type ont été abondamment étudiés par B. SEGRE et son école (cf. notamment [1], [6], [7]). On leur doit en particulier le

THÉORÈME 5 (SEGRE-BARLOTTI). - *Si* $p \neq 2$, *une* $(q + 1)$-*calotte dans* $E_{2,q}$ *est une conique, une* $(q^2 + 1)$-*calotte dans* $E_{3,q}$ *est une quadrique, et il n'existe pas de* $(q^{r-1} + 1)$-*calotte dans* $E_{r,q}$ *pour* $r > 3$.

En caractéristique 2, la situation est plus compliquée. Dans $E_{2,q}$ il existe des $(q + 1)$-calottes qui ne sont pas des coniques (par exemple l'ensemble formé de q points d'une conique et du point de rencontre des tangentes de celle-ci). L'exemple de Γ montre qu'il existe aussi, dans $E_{3,q}$, des $(q^2 + 1)$-calottes qui ne sont pas des quadriques (l'exemple donné par B. SEGRE dans [7] pour $q = 8$ est un cas particulier de celui-ci (7)). Mentionnons encore le résultat suivant, (non publié), dû à l'auteur :

PROPOSITION 2. - *Soit* Γ *une* $(q^{r-1} + 1)$-*calotte dans* $E_{r,q}$ $(q = 2^n)$. *Supposons qu'il existe sur* Γ *un point* $\underset{\sim}{\infty}$ *tel que le groupe des projectivités conservant* Γ *et ce point possède un sous-groupe invariant simplement transitif sur* $\Gamma - \{\underset{\sim}{\infty}\}$, *et au moins un sous-groupe cyclique d'ordre* $q - 1$. *Alors* $r = 2$ ou 3. *Si* $r = 2$, Γ *est, dans un système de coordonnées affines* x, y *convenablement choisi, une "courbe" d'équation* $y = x^\sigma$ *complétée par le "point à l'infini sur l'un des axes de coordonnées",* σ *désignant n'importe quel automorphisme de* K *ayant* 1 *pour seul point fixe. Si* $r = 3$, Γ *est soit une quadrique, soit l'ensemble défini au numéro* 4.2.

5. *Une définition géométrique de* G_2^*.

On peut donner pour G_2 en caractéristique 3 des résultats tout à fait parallèles à ceux des numéros 4.1 à 4.3. On se bornera à en indiquer les grandes lignes. Tout ce qui suit résulte d'ailleurs de calculs élémentaires.

Soient K un corps de caractéristique 3, $p(x_*, x_0, x_1, x_2, x_{0'}, x_{1'}, x_{2'})$ un

---

(7) Remarque communiquée à l'auteur par Mlle FELLEGARA.

espace projectif à 6 dimensions sur K , E l'hyperquadrique d'équation $x_*^2 + \sum_{i=0}^{2} x_i \cdot x_{i'} = 0$, L l'ensemble de droites (appartenant toutes à E) défini par les équations

$$(5.1) \qquad \begin{cases} p_{*i} + p_{(i+1)'(i+2)'} = 0 \\ p_{*i'} + p_{(i+1)(i+2)} = 0 \\ \sum_{i=0}^{2} p_{ii'} = 0 \end{cases}$$

(i = 0 , 1 , 2 ; les calculs sur indices se font mod 3) ,

$G(E , L)$ le groupe des projectivités de P conservant L (donc aussi E) (groupe G_2 du Tôhoku sur K) et V la variété à 5 dimensions représentant L dans l'espace projectif à 13 dimensions $D(p_{*i} , p_{*i'} , p_{ij'} , (\Sigma p_{ii'} = 0))$.

Sur V , p_{*i}^3 , $p_{*i'}^3$ et $p_{ii'}^3$ sont des polynômes en les $p_{ij'}$ $(i \neq j)$ et $p_{00'} - p_{11'}$ $(= p_{11'} - p_{22'} = \cdots)$, lesquels satisfont d'autre part à la relation

$$(p_{00'} - p_{11'})^2 + p_{01'} \cdot p_{10'} + p_{12'} \cdot p_{21'} + p_{20'} \cdot p_{02'} = 0 \quad .$$

Cela permet de définir une injection "rationnelle" ("projection" à partir de la variété linéaire $\Lambda \equiv p_{ij'} = p_{00'} - p_{11'} = 0 \quad (i \neq j')$

$$(5.2) \qquad (p_{*i} , p_{*i'} , p_{ij'}) \rightsquigarrow (y_* = p_{00'} - p_{11'} , y_i = p_{(i+1)i'} , y_{i'} = p_{i(i+1)'})$$

de V dans une hyperquadrique $F \equiv y_*^2 + \Sigma y_i \cdot y_{i'} = 0$, d'un espace projectif $Q(y_* , y_i , y_{i'})$ à 6 dimensions. On désignera par q_{*i} , $q_{*i'}$, etc., les coordonnées de Plücker des droites de Q . Si $(x_* , x_i , x_{i'})$ est un point de E , l'ensemble des droites de L qui passent par ce point a pour image dans Q (par l'intermédiaire de (5.2)) une droite appartenant à l'ensemble M défini par les relations (5.1) où on remplace p par q , et telle que

$$q_{00'} - q_{11'} = x_*^3 , \qquad q_{(i+1)i'} = x_i^3 , \qquad q_{i(i+1)'} = x_{i'}^3 \quad .$$

Ainsi se trouvent à nouveau définies deux injections $\delta : L \to F$ et $\delta' : E \to M$ établissant une sorte de dualité entre (E , L) et (F , M) . On peut alors, exactement comme au paragraphe 4, définir le groupe $G(F , M)$, le monomorphisme $\delta^* : G(E , L) \to G(F , M)$ (dont l'existence résulte immédiatement du fait, aisément vérifiable, que les projectivités de D induites par les éléments de $G(E , L)$ laissent invariantes Λ), et, si le Frobenius de K possède une racine carrée σ, la "polarité"

$$f : (x_* , x_i , x_{i'}) \rightsquigarrow (y_* = x_*^\sigma , y_i = x_i^\sigma , y_{i'} = x_{i'}^\sigma) ,$$

le monomorphisme $f^* : G(E , L) \to G(F , M)$, l'ensemble Γ , les groupes $G^*(f)$ et G^*. Le point $\underset{\sim}{\infty}$ de coordonnées $x_* = x_0 = x_1 = x_{i'} = 0$ appartient à Γ et l'ensemble $\Gamma - \{\underset{\sim}{\infty}\}$, qui est entièrement disjoint de l'hyperplan $x_{2'} = 0$, a pour équations, en coordonnées non homogènes

$$(x , y , z , u , v , w) = (x_1/x_{2'} , x_0/x_{2'} , x_*/x_{2'} , x_{0'}/x_{2'} , x_{1'}/x_{2'} , x_2/x_{2'}) ,$$

$$(5.3)\qquad \begin{cases} u = x^2 y - xz + y^\sigma - x^{\sigma+3} \\ v = x^\sigma y^\sigma - z^\sigma + xy^2 + yz - x^{2\sigma+3} \\ w = xz^\sigma - x^{\sigma+1} y + x^{\sigma+3} y + x^2 y^2 - y^{\sigma+1} - z^2 + x^{2\sigma+4} . \end{cases}$$

Les projectivités suivantes appartiennent à G :

$$t_{a,b,c} : (x , y , z , \ldots)$$

$$\rightsquigarrow (x + a , y + a^\sigma x + b , z - ay + bx - a^{\sigma+1} x + c , \ldots) \qquad (a , b , c \in K)$$

(on laisse au lecteur le soin de compléter la définition en exprimant que (5.3) est conservé)

$$h_k : (x , y , z , u , v , w) \rightsquigarrow (kx , k^{\sigma+1} y , k^{\sigma+2} z , k^{\sigma+3} u , k^{2\sigma+3} v , k^{2\sigma+4} w)$$
$$(k \in K^*)$$

$$\omega : (x_* , x_i , x_{i'}) \rightsquigarrow (x_* , \varepsilon_i x_{i'} , \varepsilon_i x_i) \qquad (\varepsilon_0 = \varepsilon_1 = -\varepsilon_2 = 1) ,$$

et on a le

THÉORÈME 6. – G^* _est doublement transitif sur_ Γ . _Si_ K _a plus de trois éléments, il est engendré par les_ $t_{a,b,c}$ $(a , b , c \in K)$, h_k $(k \in K^*)$ _et_ ω . _Tout élément de_ G^* _peut être mis, d'une et une seule façon, sous l'une des deux formes_ $t_{a,b,c} \cdot h_k$ _ou_ $t_{a,b,c} \cdot h_k \cdot \omega \cdot t_{a_1,b_1,c_1}$.

COROLLAIRE. - $G^*(f) = G^*$.

REMARQUES.

1. - Les déterminants de $t_{a,b,c}$, h_k et ω sont des puissances 7e, donc G^* est un sous-groupe de $PSL_7(K)$, ce qui est d'ailleurs déjà vrai (et bien connu) pour $G(E , L)$.

2. - Il n'est pas douteux que, comme B_2^* et G_2^* , F_4^* peut être défini comme le groupe des éléments de F_4 (du Tôhoku) qui "conservent" une "polarité" de la géométrie associée à celui-ci (cf. [10], notamment le paragraphe 11), et que les éléments de la géométrie incidents à leur "polaire" constituent l'octogone généralisé dont il a été question au paragraphe 2.

6. Une classe de groupes doublement transitifs.

Soient G un groupe doublement transitif de permutations d'un ensemble Γ tel que le sous-groupe laissant fixe un point ∞ de Γ possède un sous-groupe invariant U_+ , simplement transitif sur $\Gamma - \{\infty\}$, 0 et e deux points de $\Gamma - \{\infty\}$, H le groupe des éléments de G conservant ∞ et 0 , U_- le conjugué de U_+ qui a 0 pour point fixe, G_0 le groupe engendré par U_+ et U_- , $H_0 = H \cap G_0$, t l'élément de U_+ qui transforme e en 0 , $\bar{t}$ l'élément de U_- qui transforme ∞ en e , t' l'élément de U_+ qui transforme 0 en $\bar{t}^{-1}(\infty)$, et ω la transformation $t.\bar{t}.t' \in G_0$, qui échange 0 et ∞ .

Le groupe G_0 est manifestement transitif sur Γ ; il contient donc tous les conjugués de U_+ dans G . C'est par conséquent le plus petit sous-groupe invariant de G contenant U_+ .

U_+ étant simplement transitif sur l'ensemble $\Gamma - \{\infty\}$, on peut munir celui-ci d'une structure de groupe "abstrait" U (qui sera notée additivement) ayant 0 pour élément neutre et telle que $U = \{t_a , a \in U\}$, avec

$$t_a : x \rightsquigarrow a + x \qquad (x \in \Gamma) \tag{6.1}$$

(on pose $a + \infty = \infty$) . Les éléments de H sont des automorphismes de U ; l'action de H sur U sera notée multiplicativement (i. e. on posera $hx = h(x)$). On voit aisément que G (resp. G_0) se compose des transformations

$$t_a.h : x \rightsquigarrow a + hx \qquad (a \in U) \tag{6.2}$$

$$t_a.\omega.t_b.h : x \rightsquigarrow a + \omega(b + hx) \qquad (a , b \in U) , \tag{6.3}$$

avec $h \in H$ (resp. H_0) . La transformation $\omega^2 = \varepsilon$ appartient à H_0 , et on peut donc écrire

(6.4) $$\omega(\omega(x)) = \varepsilon x \qquad (\varepsilon \in H_0) \quad .$$

Si on désigne par $\bar{h}$ le transformé de $h \in H$ par ω , on a

(6.5) $$\omega(hx) = \bar{h}\omega(x) \quad .$$

Reprenant la définition de t , $\bar{t}$ et t' , on voit que $t = t_{-e}$, $\bar{t} = \omega^{-1}.t_{\omega(e)}.\omega$ et $t' = t_{e'}$, avec $e' = \omega^{-1}(-\omega(e))$. Tenant compte de $t.\bar{t}.t' = \omega$, on trouve alors la relation $\omega.t_e.\omega = t_{\omega(e)}.\omega.t_{e'}$. De façon générale, considérons, pour tout $a \in U$, les transformations $\omega.t_a.\omega$ et $t_{\omega(a)}.\omega.t_{a'}$, avec $a' = \omega^{-1}(-\omega(a))$; elles transforment toutes deux ∞ en $\omega(a)$ et 0 en 0 , donc leur quotient est un élément ρ_a de H_0 , ce qu'on peut écrire

(6.6) $$\omega(a + \omega(x)) = \omega(a) + \omega(\omega^{-1}(-\omega(a)) + \rho_a x) \qquad (\rho_a \in H_0) \ ;$$

en particulier,

(6.7) $$\rho_e = 1 \quad .$$

Notons encore qu'en posant $x = \omega^{-1}(a)$ dans (6.6), il vient

(6.8) $$\rho_a.\omega^{-1}(a) = \omega^{-1}(-\omega(a)) \quad .$$

Soit H_1 le groupe engendré par les ρ_a , les $\bar{\rho}_a$ et ε . Il est clair que $H_1 \subseteq H_0$. D'autre part, on vérifie aisément que les transformations (6.2) et (6.3), avec $h \in H_1$, forment un groupe qui contient évidemment U_+ et U_- , donc G_0 . Il s'ensuit que $H_0 = H_1$.

Un calcul élémentaire montre que les résultats précédents admettent une réciproque. De façon précise, on a le

THÉORÈME 7. - <u>Soient</u> U <u>un groupe noté additivement,</u> H <u>un groupe d'automorphismes de</u> U <u>et</u> ω <u>une permutation de</u> $U - \{0\}$. <u>Supposons qu'il existe une permutation</u> $h \rightsquigarrow \bar{h}$ <u>de</u> H , <u>une application</u> $\rho : U - \{0\} \to H$ <u>et des éléments</u> $\varepsilon \in H$ <u>et</u> $e \in U - \{0\}$, <u>tels qu'on ait les identités</u> (6.4), (6.5), (6.6) <u>et</u> (6.7) <u>pour tous</u> $h \in H$ <u>et</u> $a , x \in U - \{0\}$ $(a \neq -\omega(x))$, <u>et soit</u> H_0 <u>le sous-groupe de</u> H <u>engendré par les</u> ρ_a , <u>les</u> $\bar{\rho}_a$ $(a \in U - \{0\})$ <u>et</u> ε . <u>Désignons encore par</u> $\Gamma = U \cup \{\infty\}$ <u>l'ensemble obtenu en adjoignant un point</u> ∞ <u>à</u> U , <u>et posons</u> $a + \infty = h\infty = \omega(0) = \infty$ $(a \in U , h \in H)$, <u>et</u> $\omega(\infty) = 0$. <u>Alors, les transformations</u>

de Γ définies par (6.2) et (6.3), avec $h \in H$ (resp. H_0) forment un groupe doublement transitif. Les transformations (6.1) forment un sous-groupe invariant U_+ du groupe des éléments de G qui conservent ∞. G_0 est le plus petit sous-groupe invariant de G qui contient U_+ ; il est engendré par deux quelconques des conjugués de U_+ dans G. H_0 est un sous-groupe invariant de H et $G/G_0 \cong H/H_0$. Enfin, on peut obtenir de cette façon tout groupe doublement transitif, tel que le sous-groupe obtenu en fixant un point possède un sous-groupe invariant simplement transitif sur l'ensemble où opère le groupe, moins le point en question.

EXEMPLES.

1. - Soient K un corps, $U = K^+$ (groupe additif), $H = K^*$ (opérant de la façon évidente sur H) et $\omega(k) = -k^{-1}$, d'où $\bar{k} = k^{-1}$, $\rho_k = k^2$ et $H_0 = K^{*2}$. Alors, $G = PGL_2(K)$ et $G_0 = PSL_2(K)$.

2.-Soient K un corps de caractéristique 2 dont le Frobenius possède une racine carrée σ, $U = \{(x, y) \mid x, y \in K\}$ avec la loi de groupe

$$(x , y) + (x' , y') = (x + x' , y + y' + x^\sigma x') ,$$

$H = K^*$, opérant sur U de la façon suivante :

$$k.(x , y) = (kx , k^{\sigma+1} y) ,$$

et, en posant $(x , y) = a$, $\omega(a) = (\frac{y}{z(a)} , \frac{x}{z(a)})$ avec $z(a)$ défini par (4.2.1), d'où $\bar{k} = k^{-1}$, $\rho_a = (z(a))^{2-\sigma}$ [9] et $H_0 = K^{*2-\sigma} = K^{*\sigma}$. Alors G et G_0 sont les groupes $G^*(=B_2^*)$ et G_0^* du paragraphe 4.

3. - Soient K un corps de caractéristique 3 dont le Frobenius possède une racine carrée σ, $U = \{(x , y , z) \mid x , y , z \in K\}$ avec la loi du groupe

$$(x , y , z) + (x' , y' , z') = (x + x' , y + y' + x^\sigma x' , z + z' - xy' + yx' - x^{\sigma+1} x'),$$

$H = K^*$, opérant sur U de la façon suivante,

$$k.(x , y , z) = (kx , k^{\sigma+1} y , k^{\sigma+2} z) ,$$

et, en posant $a = (x , y , z)$, $\omega(a) = (-\frac{v(a)}{w(a)} , -\frac{u(a)}{w(a)} , -\frac{z}{w(a)})$, avec $u(a)$,

[9] ρ_a se calcule aisément en égalant les z des deux membres de (6.8), et un faisant usage des identités suivantes, faciles à établir : $z(-a) = z(a)$, $z(\omega(a)) = z(a)^{-1}$, $z(ka) = k^{\sigma+2} z(a)$.

$v(a)$ et $w(a)$ définis par (5.3), d'où $\bar{k} = k^{-1}$, $\rho_a = w(a)^{2-\sigma}$ [10], $H_0 = M^{2-\sigma}$, où M désigne le sous-groupe de K^* engendré par tous les $w(a)$. Alors, G est le groupe $G^*(= G_2^*)$ du paragraphe 5. En remarquant que $2 - \sigma$ est un automorphisme de K^* (puisque $(2 - \sigma)(2 + \sigma) = 1$), on voit que $G/G_0 \cong H/H_0 \cong K^*/M$.

REMARQUE. - Le théorème 7 et les données précédentes fournissent une définition tout à fait élémentaire des groupes B_2^* et G_2^*, mais pour montrer l'existence des groupes définis de cette façon, il faut vérifier que les conditions (6.4) à (6.7) sont satisfaites, ce qui est fort long.

PROPOSITION 3. - *Si un sous-groupe invariant de G_0 contient U_+, il coïncide avec G_0.*

Cela résulte du fait que, G_0 étant transitif sur Γ, les conjugués de U_+ dans G_0 sont tous les conjugués de U_+ dans G.

PROPOSITION 4. - *Si H est commutatif, H_0 contient tous les éléments de la forme $\bar{h}.h^{-1}$.*

En effet, puisque $G/G_0 \cong H/H_0$ est commutatif, G_0 contient le groupe dérivé de G., or $\bar{h}h^{-1}$ n'est autre que le commutateur de ω et h.

THÉORÈME 8. - *Si H_0 est commutatif et s'il existe au moins un élément $h \in H_0$ tel que l'équation $x - \bar{h}.h^{-1}.x = a$ ait une solution pour tout $a \in U$, alors G_0 est simple. Si en outre H est commutatif, G_0 est le groupe dérivé de G.*

DÉMONSTRATION. - Soit J un sous-groupe invariant non trivial de G. Celui-ci étant doublement transitif, J renferme au moins une transformation transformant 0 en ∞, soit $x \rightsquigarrow a + h_1.\omega(x)$ $(h_1 \in H_0)$. Si H_0 est commutatif, le commutateur de $x \rightsquigarrow hx$ $(h \in H_0)$ et de cette transformation est de la forme $x \rightsquigarrow b + \bar{h}.h^{-1}.x$. Si h satisfait à la condition de l'énoncé, cette dernière transformation possède au moins un point fixe en dehors de ∞, et elle est transformée en $\bar{h}.h^{-1} : x \rightsquigarrow \bar{h}.h^{-1}.x$ par toute transformation de G_0 qui conserve ∞ et qui amène ce point fixe en 0. Enfin, le commutateur de $\bar{h}.h^{-1}$ et de t_c (cf. (6.1)) est t_d, avec $d = c - \bar{h}.h^{-1}.c$. Mais, en vertu de l'hypothèse faite sur h, lorsque c parcourt U, il en est de même de d. Par conséquent, J contient U_+ et $J = G_0$ en vertu de la proposition 3. La seconde partie de l'énoncé résulte de la simplicité de G_0 et de la relation $G/G_0 \cong H/H_0$.

---

[10] On égale les z des deux membres de (6.8) et on fait usage des identités : $z(-a) = -z(a)$, $w(-a) = w(a)$, $z(\omega(a)) = -z(a).w(a)^{-1}$, $w(\omega(a)) = w(a)^{-1}$, $z(ka) = k^{\sigma+2}\, z(a)$.

Le théorème 8 a pour conséquence immédiate la partie du théorème 1 qui concerne B_2^* et G_2^*. Notons encore le

COROLLAIRE (SUZUKI). - Soit G un groupe doublement transitif de permutations d'un ensemble fini Γ de $2m + 1$ point. Si G renferme des permutations différentes de l'identité ayant deux points fixes, et si, par contre, l'identité est la seule permutation appartenant à G qui possède plus de deux points fixes, G est simple.

DÉMONSTRATION. - Le sous-groupe G_∞ de G formé par les éléments de ce groupe qui laissent fixe un point $\infty \in \Gamma$ donné est un groupe de Frobenius, donc les éléments de G_∞ qui ne laissent fixe aucun point en dehors de ∞ constituent un sous-groupe invariant U_+ de G_∞, simplement transitif sur $\Gamma - \{\infty\}$. On peut donc appliquer les considérations qui précèdent. Une transformation appartenant à G et échangeant 0 et ∞ ne peut avoir un cycle d'ordre impair > 1, sinon une puissance de cette transformation aurait plus de 2 points fixes sans être l'identité ; il en résulte que cette transformation possède exactement un point fixe, donc que son carré est l'identité. Soient ω et H définis comme plus haut, h_1 et h_2 deux éléments de H et $\omega_i = h_i\,\omega$ $(i = 1\ ,\ 2)$. Les transformations ω_1, ω_2, $\omega.\omega_1.\omega$ et $\omega_1.\omega.\omega_2$, qui échangent toutes 0 et ∞, sont involutives. Il en résulte que

$$h_1\,h_2 = \omega_1.\omega.\omega_2.\omega = (\omega_1.\omega.\omega_2)^{-1}\,\omega = \omega_2.\omega.\omega_1.\omega = h_2\,h_1\ ,$$

c'est-à-dire que H est commutatif, et

$$\bar{h}_1 = \omega.h_1.\omega = \omega.\omega_1.\omega.\omega = \omega.\omega_1 = h_1^{-1}\ .$$

L'ordre de H divise $2m - 1$ (puisque, par hypothèse, H est simplement transitif sur ses orbites différentes de $\{0\}$ et $\{\infty\}$) ; il est donc impair. Il en résulte que tout élément de H est un carré, donc est de la forme $\bar{h}.h^{-1}$, et on a $G = G_0$, en vertu de la proposition 4.

D'autre part, quels que soient $x\ ,\ x' \in \Gamma - \{\infty\}$ et $h \in H$ $(h \neq 1)$, l'égalité $x - hx = x' - hx'$ entraîne $-x' + x = h.(-x' + x)$, d'où $x = x'$; en d'autres termes, l'application de $\Gamma - \{\infty\}$ dans lui-même définie par $x \rightsquigarrow x - hx$ est injective, donc bijective ; et on est dans les conditions d'application du théorème 8. Le corollaire est ainsi démontré.

REMARQUE. - Le groupe B_2^* sur un corps K fini satisfait aux conditions de l'énoncé précédent.

BIBLIOGRAPHIE

[1] BARLOTTI (Adriano). - Un'estensione del teorema di Segre-Kustaanheimo, Boll. Unione mat. Italiana, t. 10, 1955, p. 498-506.

[2] BOURBAKI (Nicolas). - Algèbre, chap. 7. - Paris, Hermann, 1948 (Act. scient. et ind., 1044 ; Eléments de Mathématique, 14).

[3] CHEVALLEY (Claude). - Sur certains groupes simples, Tôhoku math. J., Series 2, t. 7, 1955, p. 14-66.

[4] REE (Rimhak). - A family of simple groups associated with the simple Lie algebra of type (G_2) , Amer. J. of Math. (à paraître).

[5] REE (Rimhak). - A family of simple groups associated with the simple Lie algebra of type (F_4) , Amer. J. of Math. (à paraître).

[6] SEGRE (Beniamino). - Le geometrie di Galois, Annali di Mathematica, Serie 4, t. 48, 1959, p. 1-96.

[7] SEGRE (Beniamino). On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two, Acta Arithmetica, t. 5, 1959, p. 315-332.

[8] STEINBERG (Robert). - Variations on a theme of Chevalley, Pacific J. of Math., t. 9, 1959, p. 875-891.

[9] SUZUKI (Michio). - A new type of simple groups of finite order, Proc. Nat. Acad. Sc. U. S. A., t. 46, 1960, p. 868-870.

[10] TITS (Jacques). - Sur les analogues algébriques des groupes semi-simples complexes, Colloque d'Algèbre supérieure [1956. Bruxelles] ; p. 261-289. - Louvain, Ceuterick, 1957 (Centre belge de Recherches mathématiques).

[11] TITS (Jacques). - Les "formes réelles" des groupes de type E_6 , Séminaire Bourbaki, t. 10, 1957/58, n° 162, 15 p.

[12] TITS (Jacques). - Sur la trialité et certains groupes qui s'en déduisent. - Paris, Presses universitaires de France, 1959 (Inst. H. Et. scient.. Publications mathématiques, 2 ; p. 14-60).